CLAIMS:

1. A system for securing data transactions between a remote device and a host device, the remote device comprising:

an interface adapted for operative connection between the host device and the remote device;

a managing controller operatively connected to the interface, the managing controller for controlling data transactions between the remote device and host device; and,

a hardware random number generator (HRNG) controller operatively connected to the managing controller for providing non-deterministic random number data for data encryption to the managing controller.

2. A system as in claim 1wherein the HRNG controller includes an HRNG for providing streaming random number bits and the HRNG controller formats the random number bits to at least one predetermined byte format.

3. A system as in claim 1 wherein the HRNG controller includes a secured memory area.

4. A system as in claim 3 wherein the HRNG controller generates an ID number for storage in the secured memory area.

5. A system as in claim 4 wherein the ID number is encrypted to a first level with an ID decrypt key.

6. A system as in claim 5 wherein the encrypted ID number is encrypted to a second level with a public key for enrollment of the remote device with the host device.

7. A system as in claim 5 wherein the host device uses the public key to decrypt the ID number to the single level and the host device stores the first level encryption ID number.

8. A system as in claim 6 wherein the public key is changed by a system administrator.

9. A system as in claim 6 wherein after enrollment, the HRNG controller verifies the validity of the first level encryption ID number prior to an exchange of application specific data between the host and remote device.

10. A system as in claim 9 wherein upon verification of the first level encryption ID number, the HRNG controller creates a data decrypt key for encrypting application specific data to a first data encryption level.

11. A system as in claim 10 wherein the HRNG controller creates a new ID decrypt key for encrypting the ID number to a first level.

12. A system as in claim 11 wherein the application specific data encrypted to a first data encryption level and the ID number encrypted to a first level and the data decrypt key are appended to one another to form an appended data packet.

13. A system as in claim 12 wherein the appended data packet is encrypted with the public key.

14. A system as in claim 1 wherein the interface is a pass-through interface.

15. A system as in claim 1 wherein the interface is wireless.

16. A system as in claim 1 wherein the at least one pre-determined format includes at least one game-of -chance format.

17. A system as in claim 1 wherein the HRNG controller has physical and electrical intrusion detection and internal memory self-destruction responsive to physical or electrical intrusion.

18. A system as in claim 1 further comprising a biometric identification system operatively connected to the remote device.

19. A system as in claim 18 wherein the biometric identification system is selected from any one of or a combination of a voice recognition, facial recognition or finger print recognition system.

20. A system as in claim 1 wherein the remote device is stealth with respect to the host device.

21. A dongle for controlling and managing data communications between a host device and the dongle, comprising:

an interface adapted for operative connection between the host device and the dongle;

a managing controller operatively connected to the interface, the managing controller for receiving and providing data to and from the host device and for receiving and providing data to and from a hardware random number generator controller operatively connected to the managing controller, the HRNG controller for providing non-deterministic random number data to the managing controller.

22. A dongle as in claim 21wherein the HRNG controller includes an HRNG for providing streaming random number bits and the HRNG controller formats the random number bits to at least one predetermined byte format.

23. A dongle as in claim 21 wherein the HRNG controller includes a secured memory area.

24. A dongle as in claim 23 wherein the HRNG controller generates an ID number for storage in the secured memory area.

25. A dongle as in claim 24 wherein the HRNG controller encrypts the ID number to a first level with an ID decrypt key.

26. A dongle as in claim 25 wherein the HRNG controller encrypts the encrypted ID number to a second level with a public key during enrollment of the remote device with the host device.

27. A dongle as in claim 26 wherein after enrollment, the HRNG controller verifies the validity of the first level encryption ID number prior to an exchange of application specific data between the host and remote device.

28. A dongle as in claim 27 wherein upon verification of the first level encryption ID number, the HRNG controller creates a data decrypt key for encrypting application specific data to a first data encryption level.

29. A dongle as in claim 25 wherein the HRNG controller creates a new ID decrypt key for encrypting the ID number to a first level for each exchange of application specific data.

30. A dongle as in claim 28 wherein the application specific data encrypted to a first data encryption level and the ID number encrypted to a first level and the data decrypt key are appended to one another to form an appended data packet.

31. A dongle as in claim 30 wherein the appended data packet is encrypted with the public key.

32. A dongle as in claim 21 wherein the interface is a pass-through interface.

33. A dongle as in claim 21 wherein the interface is wireless.

34. A dongle as in claim 21 wherein the at least one pre-determined format includes at least one game-of -chance format.

35. A dongle as in claim 21 wherein the HRNG controller has physical and electrical intrusion detection and internal memory self-destruction responsive to physical or electrical intrusion.

36. A dongle as in claim 21 further comprising a biometric identification system operatively connected to the remote device.

37. A dongle as in claim 36 wherein the biometric identification system is selected from any one of or a combination of a voice recognition, facial recognition or finger print recognition system.

38. A dongle as in claim 21 wherein the dongle is stealth with respect to the host device.

39. A method of enrolling a specific remote device with a host device comprising the steps of:

a. generating and storing a non-deterministic ID number in the remote device;

b. encrypting the ID number to a first level with a non-deterministic ID decrypt key;

c. encrypting the first level encrypted ID number to a second level with a public key;

d. passing the second level encrypted ID number to the host device;

e. decrypting the second level encrypted ID number in the host device with the public key to the first level and storing the first level encrypted ID number in the host device.

40. A method of verifying the enrollment of a specific remote device with a host device comprising the steps of:

a. requesting a first level encrypted non-deterministic ID number from the host device by the remote device;

b. receiving and decrypting the first level encrypted non-deterministic ID number with a previously generated and stored non-deterministic ID decrypt key; and,

c. verifying equivalency between the decrypted non-deterministic ID number of step b) with a previously generated and stored non-deterministic ID number in the remote device.

41. A method of transferring data between a remote device previously enrolled with a host device comprising the steps of:

a. encrypting a data packet with a non-deterministic data decrypt key;

b. encrypting an ID number with a non-deterministic ID decrypt key;

c. appending the encrypted data packet of step a) to the encrypted ID number of step b) with the ID decrypt key of step b) to form an encrypted data packet;

d. encrypting the encrypted data packet of step c) with a public key to form a second level encrypted data packet;

e. passing the second level encrypted data packet to the host device; and,

f. decrypting the second level encrypted data packet of step e) with the public key and data decrypt key to retrieve the data packet.

42. A method as in claim 41 wherein the encrypted ID number of step b) updates a previously stored encrypted ID number in the host device.

43. A system for enrolling a user with a service provider to allow access to the service provider from a non-secure location comprising the steps of:

at a secure or non-secure location for enrolling the user,

a) providing a user with a character personal identification number (PIN);
b) providing a user with a voice PIN;
c) having a user speak the voice PIN into a voiceprint processor to create a secure-location voice print file of the voice PIN;
d) storing the character PIN and voice print file in an authorized user database.

44. A system as in claim 43 further comprising the steps of:

at a non-secure location having a computer and a second voice print processor operatively connected to the authorized user database,
a) prompting a user to enter the character PIN;
b) prompting a user to enter the voice PIN into the second voice print processor to create a non-secure location voice print file;
c) submitting the character PIN and non-secure location voice print file to the authorized user database; and,

at the authorized user database
d) searching the character PIN in the authorized user database for similar character PINs; and

e) searching the non-secure location voice print file against the voice print files of record for similar character PINs to determine if the non-secure location voice print file corresponds to a voice print file of record.

45. A system as in claim 44 further comprising the step of notifying the user if they are an authorized or unauthorized user.

46. A system as in claim 45 further comprising the step of periodically requesting re-entry of the character PIN and voice PIN for re-authorization if the user is an authorized user and has gained access to the service provider's services.

47. A system as in claim 43 wherein at enrollment and prior to step a), the user declares if they meet specific enrollment criteria for accessing the service provider.

48. A method for enrolling and securing transactions between host devices each having a dongle as in claim 21 and a central enrollment database comprising the steps of:

a. enrolling an encrypted ID# within the dongle with the central enrollment database; and,

b. verifying each host device has completed the enrollment of step a) prior to permitting a public key encrypted transaction between the host devices.